Start Your SASE Journey with Cloud SWG

Table of Contents

The Shift to Hybrid Workers and Cloud Apps

Over the past few years, an increasing number of workers have relocated from the corporate headquarters to remote and home office locations, causing new challenges for network and security teams worldwide. Organizations have embraced the new normal, and it seems that the hybrid work model is here to stay, with 76% of employees wanting to continue working from home at least part of the time.[1]

It's not just the workers that are remote, however. The rapid growth of software-as-a-service (SaaS) has contributed to a high percentage of applications that are now based in the cloud. As a result, the majority of workers and the applications they access now reside outside the traditional data center walls. The world wide web has become the new network perimeter.

Web Proxy Appliances Can't Keep Up

This new paradigm can be especially challenging when an organization relies on multivendor on-premises security appliances that were never designed for today's cloud-centric world and global hybrid users. According to a survey by industry analyst Enterprise Strategy Group (ESG Global), when asked "What are the biggest challenges your organization faces relative to access control and management network security tools?" the leading responses include:[2]

- Inconsistent management across physical and cloud/virtual environments
- Introduce performance issues that negatively impact user experience
- Too many disparate tools
- Difficult to implement

Additional research from ESG Global shows that many organizations are open to a new approach to secure web gateway, with only 8% of research respondents indicating they are very satisfied with their current solution and not planning to change anytime soon.[3]

Some of the key limitations associated with traditional on-premises web proxy appliances include:

- **Incomplete security**: On-premises web proxy appliances and other multivendor legacy products were never designed for the cloud and fail to provide complete, consistent security across all users, locations, and devices.
- **Limited app coverage**: More than half of all remote workforce threats are for non-web apps, which are invisible to web proxies. Security teams can't block what they can't see, so the risk of a data breach increases without security for both web and non-web apps.
- **Poor end-user experience**: Performance bottlenecks result when organizations backhaul remote worker internet traffic to data center-based web proxy appliances for access and security (figure 1). In addition, remote workers often use a VPN, not an SWG, to obtain access to private applications, which can cause confusion and connectivity issues, resulting in more calls to the IT help desk.
- **Multivendor appliance limitations**: Using appliances from multiple vendors results in a lack of centralized management, inconsistent security policies, slow performance, and poor visibility into network threats across the organization (figure 2).

1. *The State of Hybrid Workforce Security 2021*, Palo Alto Networks, August 15, 2021, https://start.paloaltonetworks.com/state-of-hybrid-workforce-security-2021.
2. "Modernize Your Secure Web Gateway with SASE", Enterprise Strategy Group, January 2022, https://www.paloaltonetworks.com/resources/whitepapers/modernize-your-secure-web-gateway-with-sase.
3. Ibid.

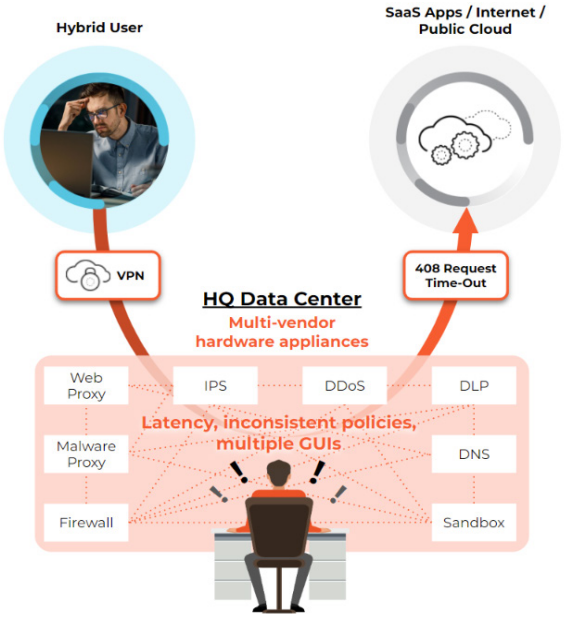


Figure 1: Backhauling traffic to the data center for access and inspection

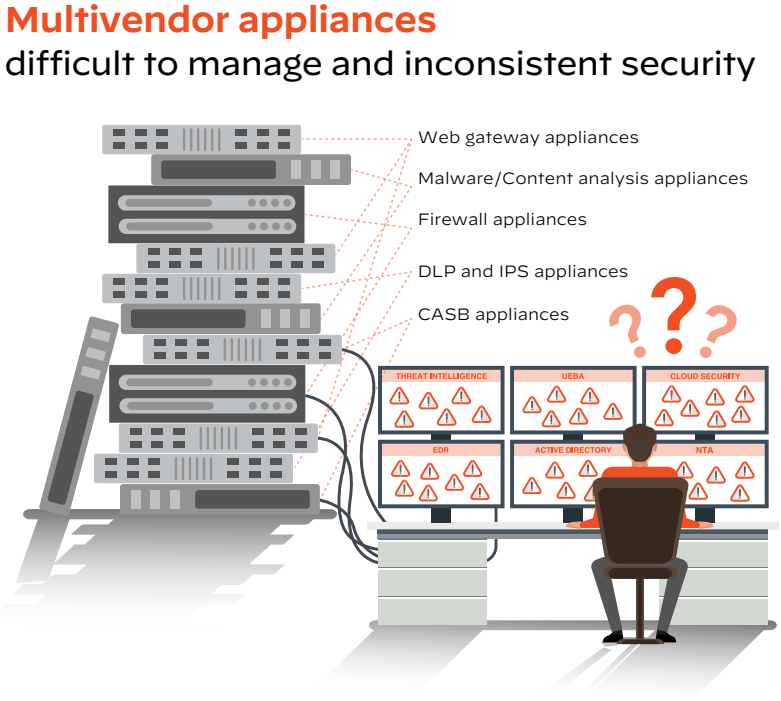


Figure 2: Multivendor security appliances

A Modern and Complete Cloud-Delivered Solution

Today, organizations require a modern web security solution that provides best-in-class threat protection—along with deep visibility, centralized management, and unified policies—to protect users, data, and applications wherever they reside. Web security is an essential part of a modern secure access service edge (SASE) architecture, so it shouldn't be managed in isolation. Palo Alto Networks Cloud Secure Web Gateway (SWG) delivers complete cloud security through Prisma Access.

Our world-class threat prevention enables you to see and protect all web traffic against malware, fileless attacks, phishing, and more. Natively integrated next-gen cloud access security broker (CASB) capabilities and enterprise data loss prevention (DLP) provide full visibility into SaaS applications to ensure your sensitive data is always protected. Combined with integrated URL filtering, malware analysis, domain name system (DNS) layer security, and remote browser isolation (RBI), we make it easy to extend consistent security to anyone, anywhere, on any device.

Our Cloud Secure Web Gateway delivers modern, complete cloud security through Prisma Access, including:

- **Protection for all app traffic**: Our Cloud SWG provides access to all apps and secures against all threats, not just web-based apps and threats; enables organizations to reduce the risk of a data breach by up to 45%.[4]
- **Complete, best-in-class security**: Industry-leading capabilities converged into a single cloud-delivered platform, providing more security coverage than any other solution. We deliver more than 4.3M unique security updates per day—24.5x more than our nearest competitor.
- **Exceptional user experience**: Our massively scalable network with ultra-low latency is backed by industry-leading SLAs to ensure the best digital experience possible for end users. We provide 10x more total encrypted tunnel throughput than the nearest competitor, and our performance SLAs are 10x better than any other cloud-delivered service.

In addition, Palo Alto Networks is the first vendor to introduce machine learning (ML)-powered security capabilities to our already impressive arsenal of best-in-class protections. Prisma Access leverages machine learning for proactive real-time and inline zero-day protection, introducing multiple industry firsts:

- Prevention of up to 95% of unknown file and web-based threats instantly with inline ML.
- Prevention of other unknown threats in near-real time using zero-delay signature updates.
- Extended visibility and security to all devices, including never-seen-before IoT devices, using ML-based detection, without the need to deploy additional sensors.
- Automated policy recommendations that save time and reduce the chance of human error.

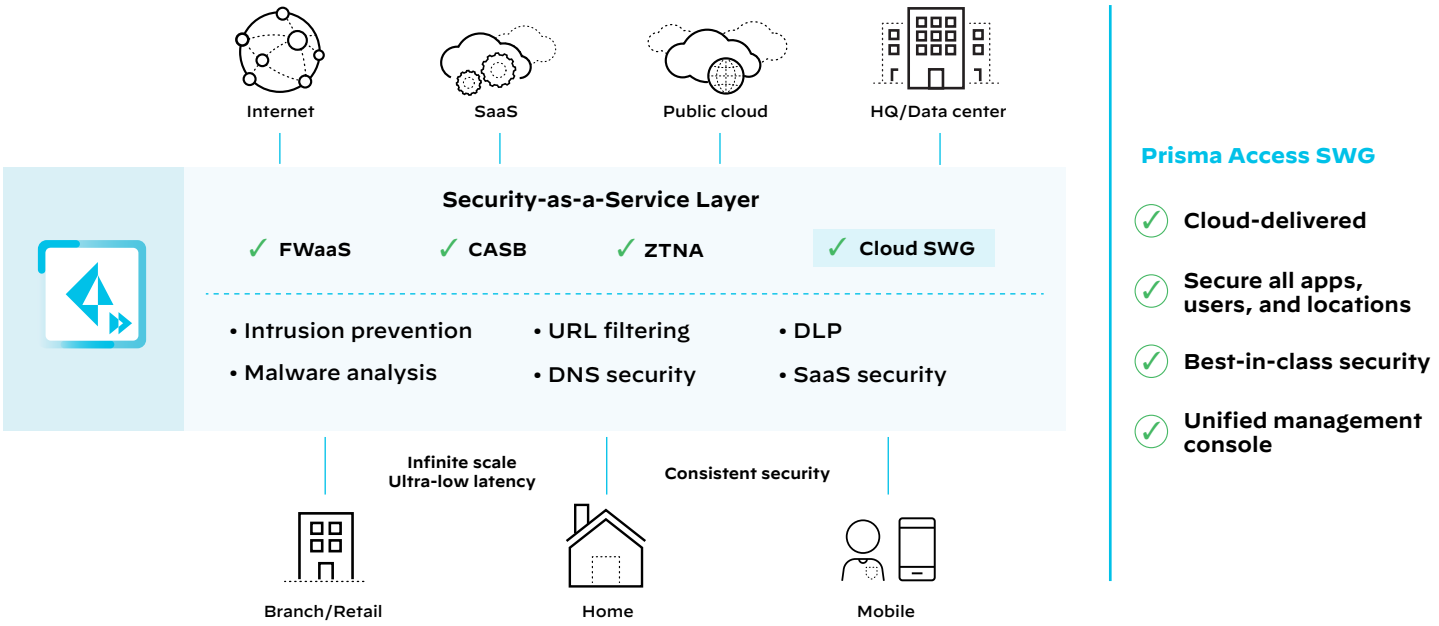


Figure 3: Palo Alto Networks Prisma Access Cloud Secure Web Gateway (SWG)

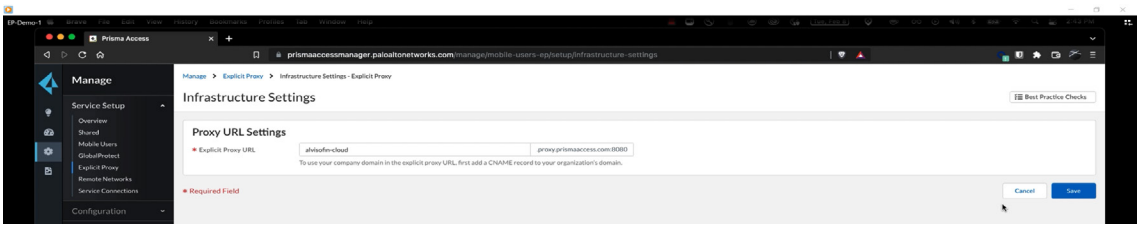
4. "Provide Secure Remote Access And Gain Peace Of Mind With Palo Alto Networks Prisma Access," a Forrester Total Economic Impact™ Spotlight commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, January 2021. https://start.paloaltonetworks.com/forrester-tei-prisma-access-spotlight.html.

Transition to Cloud Security in Just Three Steps

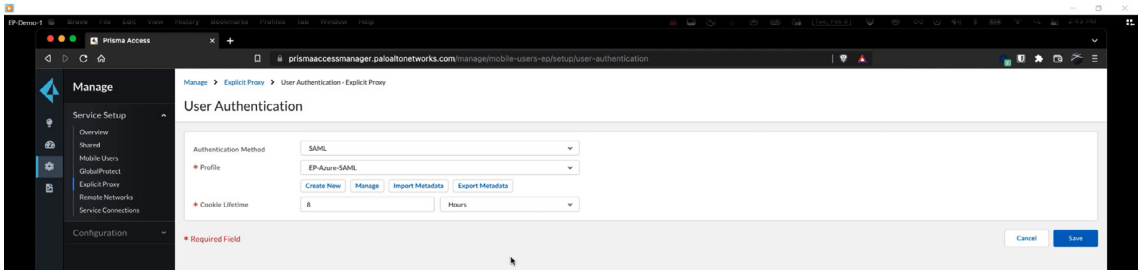
Organizations with traditional web proxy appliances can easily transition to our modern, cloud-delivered Prisma Access security platform by leveraging the cloud explicit proxy option. This approach enables existing PAC files to be quickly updated so that internet-bound traffic is directed to our cloud explicit proxy for user access and internet threat protection, without requiring any network architecture changes.

Enabling cloud explicit proxy can be accomplished in just three easy steps by utilizing Prisma Access Cloud Management. Simply configure your Infrastructure Settings, User Authentication Settings, and Prisma Access Locations. The setup process takes just a few minutes and includes an intuitive administrator interface, as shown via the sample screenshots below. Additional details are available via TechDocs online resources for cloud explicit proxy setup.

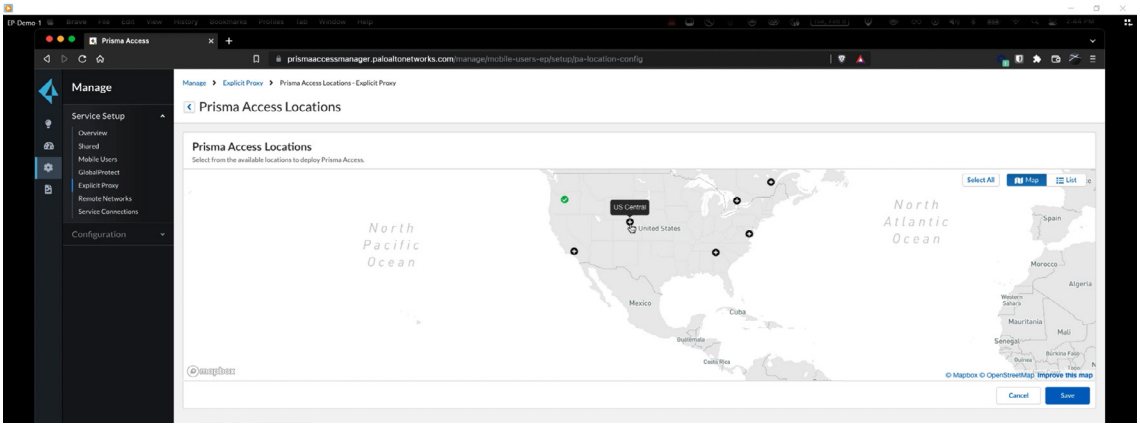
1. Infrastructure Settings



2. User Authentication Settings



3. Prisma Access Locations Settings



Prisma Access Cloud Management streamlines the setup of our cloud secure web gateway and includes a best practices dashboard, assessments, field checks, and reports to improve your security posture and increase user productivity. This enables organizations to easily and continually assess their environment via these inline checks. Best practice checks are available for the following:

- Your security policy rulebase (Note: Rulebase checks look at how security policies are organized and managed, including configuration settings that apply across many rules.)
- Security rules

- Security profiles
  - » Antispyware
  - » Vulnerability protection
  - » WildFire and antivirus
  - » URL access management
  - » DNS security
- Authentication
- Decryption
- GlobalProtect

The included best practice guidance enables organizations to simplify management and increase user productivity. By continuously assessing your configuration and policies against best practice checks, Prisma Access also allows you to take immediate action to strengthen your security posture.

In addition to our cloud explicit proxy option, Cloud Secure Web Gateway provides additional connectivity options that make it easy for organizations to protect all users and applications, wherever they reside, including:

- Managed mobile devices, which can be protected via the GlobalProtect agent to secure all ports and protocols, protecting web and non-web traffic.
- Unmanaged devices that can utilize our agentless access for full protection.
- Branch offices where users can seamlessly connect via IPsec.

An Easy Path to Complete SASE Security

The hybrid workforce and direct-to-app architectures have rendered legacy security architectures obsolete while dramatically increasing our attack surface. Cloud-based security offerings have emerged, but they can offer only inconsistent and incomplete protections as well as deliver poor performance and user experiences.

Palo Alto Networks Prisma Access protects the hybrid workforce with the superior security of ZTNA 2.0 while providing exceptional user experiences from a simple, unified security product. Purpose-built in the cloud to secure at cloud scale, only Prisma Access ZTNA 2.0 protects all application traffic with best-in-class capabilities while securing both access and data to dramatically reduce the risk of a data breach. With a common policy framework and single-pane-of-glass management, Prisma Access secures today's hybrid workforce without compromising performance. Leveraging the elastic scale of the largest cloud providers in the world, along with access to dedicated premium fiber networks, Prisma Access delivers industry-leading SLAs for security processing as well as app performance and an exceptional user experience.

In addition, Prisma Access provides a clear path for organizations that seek to implement a modern, comprehensive SASE solution. According to research from analyst ESG, *69% of research respondents indicated secure web gateway (SWG) will be the starting point or a secondary consideration for their SASE implementation.*[5] Our Cloud Secure Web Gateway seamlessly integrates with our next-generation CASB, firewall-as-a-service (FWaaS), and ZTNA 2.0 capabilities to help customers transition to a SASE model immediately. For additional insight from analyst ESG, discover how you can "Modernize Your Secure Web Gateway with SASE."

Learn how the cloud secure web gateway capabilities in Prisma Access can help your organization protect all users and applications, everywhere, today.

5. "Modernize Your Secure Web Gateway with SASE", Enterprise Strategy Group, January 2022, https://www.paloaltonetworks.com/resources/whitepapers/modernize-your-secure-web-gateway-with-sase.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com